

REMARKS

The application has been reviewed in light of the Office Action dated November 16, 2004. Claims 1-19 are pending in this application, with claims 1, 11, 12, 13, and 14 being in independent form. It is submitted that no new matter has been added and no new issues have been raised by the present Amendment.

Claim 12 was objected to because two claims contain the reference number "12." In response, Applicants have corrected this informality and changed the reference number of one of the claims to claim "10." Withdrawal of the objection to claim 12 is respectfully requested.

Claims 1-19 were rejected under 35 U.S.C. §102(b) as allegedly anticipated by U.S. Patent No. 5,826,013 to Nachenberg. Applicants have carefully considered the Examiner's comments and the cited art, and respectfully submits that independent claims 1, 11, 12, 13, and 14 are patentably distinct from the cited art, for at least the following reasons.

Independent claim 1 relates to a method of detecting a class of viral code, comprising heuristically analyzing a subject file to generate a set of flags along with statistical information, using the set of flags with statistical information to perform at least one search for a scan string and/or a statement type in the subject file, and triggering a positive detection alarm if each of the at least one search is found at least a corresponding predetermined number of times.

As described in the specification of the present application, a series of flags may be generated by the heuristic analyzer depending on the known virus (e.g., see pages 7-10). For example, as described in the specification, a typical set of flags generated by the heuristic analyzer for the W97M/Chydow.A virus may be the following:

VBA_BUILT_IN_Module_Count 1; VBA_BUILT_IN_Statement_Count 1054;

VBA_ConfirmConversions 1; VBA_InsertLines_CodeModule 1; VBA_InsertLines_Document

1; VBA_DisableVirusProtection 1; VBA_CodeModule 1; VBA_Rnd 8; and VBA_Documents_Add 1 (pages 9-10). Of course, the claims are not limited to the disclosed embodiments.

As understood by Applicants, Nachenberg relates to a polymorphic virus detection module that operates by emulating a target file by comparing each instruction from the target file with an instruction/interrupt usage profile for each known polymorphic virus. For each known polymorphic virus that does not implement the fetched instruction, a corresponding flag in a table is reset to exclude the polymorphic virus from further consideration. (Nachenberg, column 8, lines 22-37). The process of emulation continues until all mutation engines have been flagged or until a threshold number of instructions have been emulated. (Nachenberg, column 3, lines 44-46).

However, Applicants find no teaching or suggestion in Nachenberg of heuristically analyzing a subject file to generate a set of flags along with statistical information. Furthermore, Nachenberg is not understood to teach or suggest the triggering a positive detection alarm if each of the at least one search is found at least a corresponding predetermined number of times.

Accordingly, Applicants find no teaching or suggestion of heuristically analyzing a subject file to generate a set of flags along with statistical information, using the set of flags with statistical information to perform at least one search for a scan string and/or a statement type in the subject file, and triggering a positive detection alarm if each of the at least one search is found at least a corresponding predetermined number of times, as recited in independent claim 1.

Accordingly, Applicants submit independent claim 1 is patentably distinct from the cited art. Independent claims 11, 12, 13, and 14 are believed to be patentably distinct from the cited art for at least similar reasons. Withdrawal of the rejection under Section 102(b) is respectfully

requested.

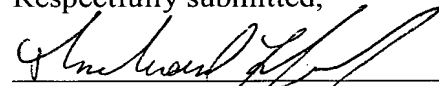
The Office is hereby authorized to charge any additional fees that may be required in connection with this amendment and to credit any overpayment to our Deposit Account No. 03-3125.

If a petition for an extension of time is required to make this response timely, this paper should be considered to be such a petition, and the Commissioner is authorized to charge the requisite fees to our Deposit Account No. 03-3125.

If a telephone interview could advance the prosecution of this application, the Examiner is respectfully requested to call the undersigned attorney.

Entry of this amendment and allowance of this application are respectfully requested.

Respectfully submitted,



RICHARD F. JAWORSKI

Reg. No. 33,515

Attorney for Applicants

Cooper & Dunham LLP

Tel.: (212) 278-0400